IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/606,089
Filing Date 06/25/2003
Inventorship ..... Christian et al.
Applicant ..... Microsoft Corp.
Group Art Unit 2137
Examiner ..... Williams, Jeffery L.
Attorney's Docket No. MS303956.01
Title: Systems and Methods for Declarative Client Input Security Screening

REPLY BRIEF

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

From: J. Richard Bucher (Tel. 509-755-7264; Fax 509-755-7252)
Sadler, Breen, Morasch & Colby, P.S.
422 W. Riverside Avenue, Suite 424
Spokane, WA 99201

Pursuant to 37 C.F.R. § 41.41, Applicant hereby submits a reply brief in application No. 10/606,089, within the requisite time of the Examiner's Answer.

REMARKS

Applicant maintains the positions set forth in the Appeal Brief, and respectfully submits that pending claims 1, 4-12, 16-21 and 24-28 are allowable.

35 U.S.C. § 102 Rejections

In the "(9) Grounds of Rejection" section of the Examiner's Answer, the Office maintains its rejections of claims 1, 4-12, 16-21 and 24-28 under 35 U.S.C. § 102(b) as allegedly being anticipated by a publication by David Scott and Richard Sharp entitled "Abstracting Application-Level Web Security" (hereinafter, "Scott"). In articulating these rejections, the Office has simply restated the rejections it presented in the final Office Action. Applicant addressed these rejections at length in Applicant's Appeal Brief and thus, in the interest of brevity, will not restate those arguments herein. Applicant maintains its arguments presented in the Appeal Brief and submits that, at least for those reasons, Scott fails to disclose the subject matter of claims 1, 4-12, 16-21 and 24-28. Applicant therefore respectfully requests that the § 102(b) rejections of these claims be overturned.

Response to Arguments

In the "(10) Response to Arguments" section of the Examiner's Answer, the Office responds to certain arguments made by Applicant in the Appeal Brief. As such, Applicant will address each of these responses in the order presented by the Office:

(i) First, with respect to Applicant's argument that Scott fails to disclose "referencing a declarative security module", the Office responds:

> ...examiner respectfully notes that page 3, col. 2, par. 2 of Scott discloses more than "merely ... a policy compiler responsible for generating SPDL code which is loaded into a security gateway which acts as a firewall". Scott discloses the determination of validation constraints and transformation rules ["client input security screens"] that are to be applied to input received from the client. This determination is made by "referencing" [see also Scott, sect. 3.3, par. 1, lines 1-3] a SPDL policy [i.e. an XML specification and corresponding DTD (the specification and DTD containing statements which declare the security screening techniques to be performed) - thus, a "declarative module"] - also see Scott, pg. 4, col. 1, par. 2; fig. 5). Therefore, Scott discloses "referencing a declarative security module".

Applicant respectfully disagrees. Applicant notes that although the Office asserts that Page 3 of Scott discloses more than a policy compiler for generating SPDL code, the Office still relies on the policy complier compiling SPDL code/specification of Scott as disclosing "referencing a declarative module..." as claimed. For example, the excerpt from Section 3.3 (Par. 1 (lines1-3)) of Scott, relied upon by the Office, states "[t]he *policy compiler* takes an SPDL specification (as described in Section 3.2) and compiles it for execution on the Security Gateway". In addition, Page 4 (Col. 1 – Para. 2) and Fig. 5 of Scott merely describe/depict elements of the SPDL code/specification. As such, Applicant maintains its arguments presented in the Appeal Brief with respect to "referencing a declarative module..." as claimed.

(ii) Second, with respect to Applicant's argument that Scott fails to disclose a declarative module comprising "a global section" as claimed, the Office responds:

> ...examiner respectfully notes that Scott discloses that the security policy comprises a section of statements for screening all client input, and thus teaches "a global section". See Scott, page 6, col. 1, par. 1, 2, par. 2, lines 9-13; fig. 2. Herein, Scott discloses input security screens (i.e. a transformation screen) that are applied to all user input (parameters values). See also, Scott, pg. 2, col. 2, "Cross-Site-Scripting" section, par. 3.

Applicant respectfully disagrees. First Applicant notes that its arguments presented in the Appeal Brief explained, at length, why Fig. 2 and Page 6 (Col. 1 – Para. 2) of Scott (and Scott in general) fails to disclose a global section ... that applies to ***any type of client input***" as this is understood in the context of the claim language (e.g., "a global section ... and an individual values section...") and the subject application. (Emphasis added). Furthermore, with respect to the cited excerpt from Page 2 (Col. 2, Section ""Cross-Site-Scripting", Para. 3) of Scott, this excerpt merely indicates that XSS vulnerabilities can be fixed by encoding XML meta-characters, that the flexibility of HTML makes this complicated and that "...for large applications, it is a laborious and error-prone task to ensure that *all* input from the user has been appropriately HTML encoded." Missing, however, is any mention of a declarative module comprising "a global section" as claimed. Furthermore, the Office reliance on this excerpt for "a global section" is logically inconsistent with its reliance on compiling SPDL code for "a declarative module". Accordingly, Applicant maintains its arguments presented in the Appeal Brief in this regard.

(iii) Third, with respect to Applicant's argument that Scott fails to disclose "first using the global section", the Office responds:

> ...examiner respectfully notes that Scott clearly discloses first using the "global section" (e.g. the encoding transformation of all input) then using "the individual values section" (i.e. validating individual parameters). For example, figure 4 distinctly shows the operational process, wherein the sequence is "Apply transformations"(FIRST) -7 "Execute Validation Code" (SECOND). Also, paragraph 3 of section 3.4 reveals the sequence of using the declared transformations and validations. Within the sequence shown in paragraph 3, the transformations occur before the validations. If one event comes before another event within a sequence, the event that comes before the other is said to be first within that sequence.

Applicant respectfully disagrees and maintains its arguments presented in the Appeal Brief. In this regard, Applicant again emphasizes that Section 3.4 (Paras. 1-3) of Scott describes Fig. 4 as first checking parameters and cookies and then ("next") applying transformations.

(iv) Fourth, with respect to Applicant's argument that Scott fails to disclose a "web.config" file, the Office responds:

> ...examiner respectfully notes that Scott discloses providing a security policy for a web application (such as a ASP or PHP applications - see Scott, sect. 3.5.2; fig. 5). The security policy comprises an XML file containing statements declaring the various transformation and validation security screens for configuring the security of a web application. Thus, Scott discloses a "web.config" file for a web application, which according to the appellants is a file comprising the security screening statements for a web application and is "designated "web.config." (See Appellants' specification, pg. 5, lines 15-23; pg. 6, line 23 - pg. 7, line 1). The examiner respectfully points out that, whether or not the appellants designate a file as "web.config" or any other name or title, there remains no structural or functional difference between the claimed file containing security screening statements and the prior art file comprising the security screening statements.

Applicant respectfully disagrees and submits that while Page 5 (lines 15-23) and Pages 6 (line 12) through 7 (line 1) of the specification indicate that a "web.config" file may contain certain entries/statements, they do not define or limit a "web.config…as/to "a file comprising the security screening statements for a web application and is designated 'web.config'". Therefore, Applicant submits that the Office is impermissibly relying on its own unsubstantiated definition for a "web.config" file as the basis for its rejection. Accordingly, Applicant maintains its arguments presented in the Appeal Brief that Scott fails to disclose or suggest a declarative module which comprises a "web.config file".

For the Office's convenience, these excerpts from Applicant's specification are reproduced below.

> As a project is created, acceptable items of client input and associated required filters are ascertained. For each item of input, there is a corresponding entry into a custom section of the file designated "web.config". This file contains general configuration information for the entire project.
>
> An exemplary portion of a web.config file is shown below. The following example will be referred to throughout the remainder of this document.

<inputValidation filter="[\<\>]" action="remove">
<queryString name="srch" filter="[%\;(){}!\n\t]" action="remove"/>
<serverVariable name]"SERVER_NAME" filter="[\w|.]+" />
</inputValidation>
Page 5 (lines 15-23)

> The server 102 also includes multiple projects 108(1) – 108(n), also referred to herein as web applications or web services and designated collectively as project 108 when appropriate. In the present example, the projects 108 are significantly generalized and may contain virtually any number of content pages or items (not shown).

Each project 108 includes a web.config file 110 that includes general configuration statements related to a specific project 108. web.config file 110(1) may be identical to or different from web.config file 110(n), depending on the particular needs of each project 108. To function appropriately within the server 102, the web.config file 110 must be included in each project 108.

Each web.config file 110 includes a client input security screening (CISS) unit 112. The CISS unit 112 may be a separate module within the web.config file 110, but will typically comprise a contiguous section of statements within the statements included in the web.config file 110. Particular elements and functions…

Pages 6 (line 12) through 7 (line 1)

(v) Fifth, with respect to Applicant's argument that Scott fails to disclose a "executing a default action" or "executing a specified action" as claimed, the Office responds:

…examiner points out that any action performed by a *designed* system, such as a computing system, is a "specified" action. In other words, a designed system depends upon the specification of the designer for operation. Thus, the actions performed by such a system (e.g. *'upon event* X *perform action* Y' or *'upon event* X *generate error'* or *'upon event* X *do something random'* or *'upon event* X *be passive/be active')* are all "specified" ways for a computer to act as determined by the designer. Throughout the disclosure of Scott, it may be seen that the system of Scott comprises the application of a plurality of client input security screens upon valid and invalid input.

Furthermore, regarding "default" actions, the examiner respectfully notes that Scott discloses an automated system (Scott, fig. 1; fig. 4). The system of Scott operates according to a defined design. Thus, the actions performed by such a system constitute a default operation of the system. While it is noted that automated systems possibly may comprise means for a user to override the default operation or actions of the system, the examiner respectfully points out that Scott does not disclose such a manual overriding of the system operation (see for example, Scott, fig. 4). Thus, the system of Scott clearly discloses "default" actions.

Applicant respectfully disagrees for the following reasons. First, the Office's argument that (a) "any action performed by a *designed* system, such as a computing system, is a "specified" action" and (b) "[t]he system of Scott operates according to a defined design…[t]hus, the [any] actions performed by such a system constitute a default operation of the system" is inconsistent with Applicant's specification. By way of example and not limitation, Fig. 3 and the accompanying discussion on Pages 9 (line 6) through 12 (line 12) describe a designated/specified action (Block 310) that is taken if Block 308 is "No" and a default action (Block 318) that is taken if Block 316 is "No". As such, *any* action in Scott cannot reasonably be equated with a "specified action" or a "default action" as those terms are used and understood in the context of Applicant's specification.

Second, with respect to dependent claims 7, 8, 25 and 26, Applicant notes that these claims recite executing "***on invalid client input***." (Emphasis Added). Accordingly, Applicant maintains its arguments presented in the Appeal Brief that it is unable to find any such actions in the cited excerpts.

(vi) Sixth, with respect to Applicant's argument that Scott fails to disclose "removing an entire string that contains the one or more screened values detected in the client input", the Office responds:

> …examiner respectfully notes that Scott discloses the encoding of all input data. Thus, Scott discloses removing all the original data and replacing the original data with substituted characters or numbers (see for example, Scott, page 6, col. 1 (lines 1-12_). As such, Scott discloses *"...removing an entire string that contains the one or more screened values detected in the client input".*

Applicant respectfully disagrees and submits that the cited excerpt on Page 6 (Col 1 (lines 1-12)) of Scott merely describes ***replacing*** (transforming) ***specific characters*** (i.e., single quotes or double quotes"), not ***removing*** an ***entire string*** that contains the one or more screened values detected in the client input. Accordingly, Applicant maintains its arguments presented in the Appeal Brief in this regard.

(vii) Seventh, with respect to Applicant's argument that Scott fails to disclose the features of claims 12, 16-20, 21 and 24-28, the Office responds:

> ...examiner respectfully notes that claims that that claims 12, 16-20, 21, and 24-28 are system and computer program claims corresponding to the method claims of 1 and 4 - 11. As the appellant repeats what are essentially the same arguments as for method claims 1 and 4 - 11, the examiner respectfully notes that such arguments regarding the system and computer program claims appear to be unpersuasive for the same reasons as shown above.

Without conceding that it "repeats what are essentially the same arguments as for method claims 1 and 4 – 11", for the sake of brevity Applicant nevertheless maintains its arguments presented in the Appeal Brief and in this Reply Brief in so far as they are germane to the Office's rejections of claims 12, 16-20, 21 and 24-28.

(viii) Eighth, with respect to Applicant's argument that Scott fails to disclose "a default action that is not required to be specified in a client input security screen", as recited in claim 26, the Office responds:

> ...examiner respectfully notes that Scott discloses an automated system that performs actions (e.g. "return error page") which are not required to be specified within a client security screen (compare, for example, to fig. 5 - wherein the example declarative module does not comprise specifying a "return error page" as is performed when certain screenings fail). (Scott, pg. 6, col. 1, par. 1, 2, col. 2; fig. 4). Thus, Scott discloses disclose "a default action that is not required to be specified in a client input security screen".

Applicant respectfully disagrees and submits that, as noted above, *any* action (e.g., "the actions") in Scott cannot reasonably be equated with a "default action" as that term is used and understood in the context of Applicant's specification. Accordingly, Applicant maintains its arguments presented in the Appeal Brief in his regard.

Conclusion

The Office's basis and supporting rationale for the rejections discussed above are not supported by the Office's arguments or the cited reference. Applicant respectfully requests that the rejections be overturned and that pending claims be allowed to issue.

Respectfully submitted,

Dated: June 7, 2008

/J. Richard Bucher/
J. Richard Bucher
Registration No. 57,971
Sadler, Breen, Morasch and Colby, p.s.
422 W. Riverside Ave., Suite 424
Spokane, WA 99201
509-755-7254